

# Digital doubters in different political and cultural contexts: Comparing citizen attitudes across three major digital technologies

Genia Kostka 

Institute for Chinese Studies, Freie Universität Berlin, Berlin, Germany  
Email: [g.kostka@fu-berlin.de](mailto:g.kostka@fu-berlin.de)

Received: 06 February 2023; Revised: 15 June 2023; Accepted: 10 July 2023

**Keywords:** contact tracing; digital technologies; facial recognition; privacy; social credit; surveillance

## Abstract



Governments all over the world are rapidly embracing digital technologies for information collection, governance, and social control. Recent studies suggest citizens may accept or even support digital surveillance. By using an online survey dataset on public opinion about facial recognition technology, contact tracing apps, and the social credit system in China, Germany, the US, and the UK, this article shows that these studies have overlooked a small yet significant group of digital technology doubters. Our results show that while up to 10% of Chinese citizens belong to the group of “digital doubters,” this group is the largest in Germany with 30% of citizens. The US and the UK are in the middle with approximately 20%. While citizens who belong to this group of digital doubters worry about privacy and surveillance issues, their attitudes can also be explained by them not being convinced of the benefits of digital technologies, including improved efficiency, security, or convenience. We find that the more citizens lack trust in their government, the more likely they are to belong to the group of digital doubters. Our findings demonstrate that in both democratic and authoritarian states, there are citizens opposing the adoption of certain digital technologies. This underscores the importance of initiating societal debate to determine the appropriate regulations that align with these societal preferences.

## Policy Significance Statement

Various countries are embracing digital technologies, but little is known about citizen attitudes and if and how they differ across digital technologies and in different political and cultural contexts. This study looks at public opinion in China, Germany, the US, and the UK and highlights commonalities and differences. Policymakers should take these attitudes on the risks and benefits of digital technologies into account when devising digital policies in their respective contexts.

## 1. Introduction

The adoption of digital technologies is expanding rapidly across the globe. Governments’ embrace of digital tools has led to innovative breakthroughs in public service delivery, efficiency gains, and new forms of citizen participation (Chadwick, 2003; Lee et al., 2011). Algorithmic decision-making processes

  This research article was awarded Open Data and Open Materials badges for transparent practices. See the Data Availability Statement for details.

often lead to more evidence-based policy (Mayer-Schönberger and Cukier, 2013; Höchtl et al., 2016; Pinker, 2018) and, thus, potentially result in fairer decisions than those formulated by persons who may be influenced by greed, prejudice, or simply incomplete information (Gandomi and Haider, 2015; Lepri et al., 2017).

At the same time, the new reliance on digital tools has also stirred social, ethical, and legal concerns about governments' extensive adoption of digital technologies. Increasing evidence points to the risks of biases, values, and ideologies being expressed through smart applications that run on flawed data inputs and algorithms (Kraemer et al., 2011; O'Neil, 2016). Algorithmic decision-making carries the biases of the human actors who construct the algorithms and lacks transparency and accountability owing to technical complexity and/or intentional secrecy or biases (Citron and Pasquale, 2014; Diakopoulos, 2015; Pasquale, 2015; Burrell, 2016; Lepri et al., 2017). Generally, the more sophisticated a technology is, the more "black-boxed" its functionality is to users and the more it lacks scrutiny from the general public (Bodo et al., 2017). Moreover, the increasing proliferation of digital devices in both public and private spaces raise unprecedented challenges concerning surveillance and defending citizens' right to privacy (Brayne, 2017; Monahan, 2018; Park, 2020).

Democratic and authoritarian states alike are incorporating digital technologies into digital governance processes. In the context of authoritarian states, recent evidence suggests that digital-based governance approaches increase the chances of regime survival by enhancing autocrats' surveillance and repression capacity while also providing new mechanisms of information collection and control (Gunitsky, 2015; Wright, 2018; Guriev and Treisman, 2019; Frantz et al., 2020; Earl et al., 2022). For instance, the Iranian and Syrian governments have adopted various digital surveillance technologies to spy on citizens they perceive as political threats (Gohdes, 2014; Gunitsky, 2015). The Singaporean People's Action Party has used digital technology to soft-sell public policies and counter anti-regime comments (Tan, 2020). Recently, the Russian regime used various forms of digital surveillance tools to suppress dissent against the war in Ukraine (Bushwick, 2022). In sum, the evidence suggests that digital technologies overwhelmingly strengthen the state rather than society as they reduce the costs for authoritarian leaders to control information and identify potential political opponents.

Despite such a haunting specter generated by digital technologies, existing studies on public opinion show high public acceptance of digital technologies, surveillance, and intrusion by the state (Su et al., 2021; Liu, 2022). While these studies are very informative in explaining this public support, which can be surprising at first sight, they ignored a small but significant social group, namely those who are suspicious of digital technologies. Here, these skeptics are referred to as *digital doubters*. Digital doubters are citizens who express unambiguous disapproval of government-led digital technologies. This study looks at citizens' attitudes toward three major digital technologies in different political contexts: social credit systems (SCSs), facial recognition technology (FRT), and contact tracing apps (CTAs), with a focus on analyzing digital doubters. Based on three separate online surveys that are combined for this analysis, this study analyzes which characteristics are shared by citizens who become digital doubters and what separates them from the vast majority of supportive citizens. Particularly, the analysis checks whether the reasons are the same as those expected in the existing literature, namely that the risks from these technologies (including surveillance, privacy violations, and discrimination) outweigh the possible benefits (e.g., improved security, governance efficiency, or simply convenience). Little is known about digital doubters in different political contexts—a gap this article wants to help narrow.

This article studies citizens' skeptical attitudes toward digital technologies in four countries: China, Germany, the UK, and the US. We selected these four countries because their governments have rolled out a variety of digital technology systems. China has most strongly embraced government applications of digital technologies by, for instance, piloting local social credit pilots in more than 60 cities (Li and Kostka, 2022), setting up highway toll booths with facial recognition cameras to detect drivers evading fares (Ji et al., 2018), or equipping schools to monitor pupil attendance (Article 19, 2021). In February 2020, at the start of the COVID-19 pandemic, China was also the first country to introduce a CTA, the China Health Code, and also used FRT to enforce quarantine rules (Roussi, 2020). In the US, the adoption of FRT and CTAs is also spreading, albeit not as fast as in China (Prakash, 2018; Harwell, 2019). In the UK, police departments have experimented with live face-tracking (Satriano, 2019), whereas in Germany,

a country where the topic of data privacy is especially prominent in public debate, FRT roll-out is limited and adoption is confined to major airports that integrate FRT for identity verification. These four countries also represent a politically diverse group: an authoritarian state, a federal parliamentary republic, a parliamentary constitutional monarchy, and a presidential republic. This mixture allows us to study different political contexts. We expect to identify overarching explanatory factors that are applicable across cases, as well as context-specific dimensions.

The results show that the number of digital doubters is not small, even in a strong authoritarian state like China. While up to 10% of Chinese citizens belong to the group of “digital doubters,” this group is the largest in Germany with 30% of citizens. The US and the UK are in the middle with approximately 20%. Numerous factors explain why digital doubters are vigilant about and suspicious of digital technologies, despite the state seeking to persuade citizens to tolerate or even welcome massive surveillance and digital technologies. Generally, citizens who belong to the group of strong doubters (i.e., strongly opposing these digital technologies) are not convinced of the effectiveness and usefulness of digital technologies, including perceived benefits such as more convenience, efficiency, or security. In the group of doubters (i.e., strongly opposing or being neutral toward these digital technologies), the doubting attitudes are also associated with concerns about technology risks, especially privacy concerns. In China, there are more doubts about visible digital technologies such as FRT than CTAs and SCSs. We find that the more citizens lack trust in their government, the more likely they are to belong to the group of digital doubters. The results demonstrate that in both democratic and authoritarian states, there are citizens opposing the adoption of certain technologies. This emphasizes the need for an urgent debate on how to regulate these technologies to ensure they align with societal preferences.

## 2. Literature Review

### 2.1. Authoritarian digital governance, public opinion, and doubters

Authoritarian rulers have traditionally used a variety of means to ensure control over the public, including repression, cooptation, surveillance, and manipulation of information (Davenport, 2007; Gerschewski, 2013). Digital technologies have helped autocrats pro-actively frame and manipulate information (Deibert, 2015; Guriev and Treisman, 2019), co-opt social media (Gunitsky, 2015), or flood the web with distracting messages (Roberts, 2018; Munger et al., 2019). Digital technologies are also used to expand the state’s capacity to monitor early protests and identify potential opponents while granting average people more freedom to access information (MacKinnon, 2011). In this sense, digital tools offer autocrats more social control at a much lower cost and reduce the likelihood of protest (Kendall-Taylor et al., 2020).

Facing both an expanding surveillance state and greater freedom to monitor or even challenge the state, citizens’ attitudes toward digital technology have become vitally important. A growing body of research on public opinion has found high public acceptance of digital technologies, surveillance, and intrusion by the state (Su et al., 2021; Liu, 2022; Xu et al., 2022). Several explanations have been proposed for why citizens strongly support their authoritarian governments and various digital technology programs. The first explanation is that while economic development enhances the immediate effect of public support for authoritarian states, but in the long run, it may also foster critical citizens. For instance, in China over the past few decades, strong support of the government as a result of economic growth has eclipsed people’s distrust of the government generated by a change in values (Wang, 2005; Holbig and Gilley, 2010). Citizens would give up privacy, freedom, and other democratic rights for economic gains. For instance, Su et al. (2021) find that in China, support for digital surveillance is positively associated with overall trust in the government and satisfaction with the regime.

The second explanation for strong support relates to increased nationalism. Online nationalism stands out as one of the most influential public opinion sentiments that can be exploited by authoritarian states. It is often agreed that the rise of nationalism in China in the post-Tiananmen era is engineered to counteract eroding communist ideology among the public (Downs and Saunders, 1999; Zheng, 1999; Zhao, 2004).

The third major explanation is security over privacy as citizens value personal and financial safety more (Yao-Huai, 2005; Wang and Yu, 2015). Recent research suggests that when people think of digital technologies, surveillance, and control are not foremost in their minds but rather notions of convenience and security (Kostka et al., 2021; Su et al., 2021). Yet, the existence of digital doubters' challenges existing theories of economic for democracy, nationalism, and security.

At the same time, public support for the state's digital tools and programs is fragile. For instance, the Chinese state is increasingly encountering social resistance to various aspects of its massive digital surveillance system. The Suzhou government, for example, faced large protests when it promoted a so-called "civility code" that was part of its local SCS system. Within a few days, this civility code had to be dropped (Chiu, 2020; Du, 2020). Similar resistance has been encountered when private companies and governments promote facial recognition. Citizens also complained and even filed lawsuits against companies who inappropriately collected their personal facial information (Huang et al., 2020). In addition, people have engineered various means to evade and counter such intensified state surveillance (Li, 2019). Generally, citizens' trust in digital governance is tightly linked to their trust in government (Srivastava and Teo, 2009). In China, for instance, citizens are generally found to have high trust in their government (Li, 2004; Manion, 2006), but recent studies show that trust is lower among the young, more educated, and economically better-off (Zhao and Hu, 2017), which suggests that public opinion can shift quickly.

## 2.2. *Cost–benefit calculus*

To understand why citizens accept the adoption of digital technologies into governance processes despite possible disadvantages, the literature finds that a major reason is citizens' risk–benefit calculations. According to the privacy calculus theory, people often weigh potential benefits and risks before deciding to disclose private information (Laufer and Wolfe, 1977).

Previous studies have shown significant variation in privacy attitudes within a society. For instance, Alan Westin's research on public perceptions of privacy in the US shows the American public has a very pragmatic approach regarding specific privacy issues (Westin, 1996). According to his surveys, 25% of the US population can be classified as "privacy fundamentalists," 18% as "privacy unconcerned," and the remaining 57% as "privacy pragmatists." Privacy fundamentalists consider privacy an inherent right that should be protected at all costs, while privacy pragmatists decide on a case-by-case basis whether to align themselves with the privacy fundamentalists or the privacy unconcerned, depending on their assessment of the trade-off between giving up their private information and gaining valuable benefits (Westin, 1996). Similarly, recent research on China shows varying privacy attitudes among different societal groups. While privacy concerns regarding data collection by the government are low among citizens, they are somewhat elevated among individuals who are not ideologically aligned with the state (Steinhardt et al., 2022). The low level of privacy concerns in China may be attributed to the absence or weakness of data protection regulations prior to the introduction of the Personal Information Protection Law in 2021. By contrast, countries like Germany and the UK had already increased citizens' awareness of privacy issues through the implementation of the General Data Protection Regulation (GDPR) laws in 2018.<sup>1</sup>

Despite privacy concerns, people tend to disclose their personal information if they think the benefits outweigh the risks (Acquisti and Grossklags, 2005; Krasnova et al., 2010). That is, they sacrifice privacy in exchange for benefits. Davis and Silver (2004) show that citizens in the US trade their civil liberties, such as those infringed by electronic surveillance, for better security and safety, especially in the aftermath of 9/11. In their study on citizens' acceptance of facial recognition technologies, Kostka et al. (2021) highlight a trade-off situation in which citizens value improved security and convenience over negative drawbacks. This research draws on the privacy calculus theory to understand why certain citizens are more dubious about certain technologies than others. To analyze citizens' cost–benefit considerations, we test the perceived benefits by using the following broader dimensions: convenience, efficiency, security,

<sup>1</sup> See Radanliev (2023) for recent updates on digital regulation in the EU, the UK, and the US.

and improved regulation (social order). The perceived costs or risks of digital technologies are tested by the following measurements: surveillance, privacy violation, discriminations and biases, commercial (mis)use, and data misuse.

### 2.3. Digital technology adoption in China, Germany, the UK, and the US

China, Germany, the UK, and the US have all experimented with and applied some or all forms of the three technologies in focus: SCS pilots, FRT, and COVID-19 CTAs. SCS pilots, which are only employed in China, have been part of the Chinese state effort to both surveil and morally educate its citizens, and their rewards and punishments for the country's citizens are based on blacklists and redlists (Creemers, 2017; Engelmann et al., 2019).<sup>2</sup> It is not a single integrated initiative but a range of fragmented ones through which the Chinese government aims to consolidate legal and regulatory compliance and improve the financial services industry (Chorzempa et al., 2018). While some scholars have shown extreme uneasiness about SCSs becoming the precursor to an Orwellian society (Chorzempa et al., 2018; Dai, 2018; Mac Sithigh and Siems, 2019), SCSs are generally supported in China among more socially advantaged citizens (wealthier, better-educated, and urban residents), who register the strongest approval of SCSs (Kostka, 2019; Liu, 2022). As of 2022, there were 62 provincial and local government-led SCS initiatives serving as pilot projects (Li and Kostka, 2022). Notable examples include the Hangzhou government's *Qianjiang Score* (钱江分), the Rongcheng government's *Rongcheng Score* (容成分), and the Fuzhou provincial government's *Jasmine Score* (茉莉分). Technological intensity varies across these SCS projects, with some adopting low-tech approaches, like in Rongcheng (Gan, 2019), while others have experimented with more advanced technologies such as facial recognition, as exemplified in Shenzhen (Creemers, 2018).

FRT adoption is widespread and has particularly high adoption rates in China, followed by the US and the UK, as well as a limited roll-out in Germany, where adoption is confined to major airports that integrate FRT for identity verification. In China, government agencies have adopted FRT for multiple purposes, including urban policing, transportation systems, digital payment systems (e.g., pension payments in Shenzhen), and the social control of Muslim Uighur monitories in Xinjiang (Mozur, 2019; Brown et al., 2021). Therefore, it is not uncommon in China to find public spaces, including public libraries, train stations, and airports, equipped with FRT (Brown et al., 2021). Commercial applications have also firmly embedded the technology in the daily lives of Chinese citizens through offerings such as online banking and commercial payment systems (e.g., Alipay's Smile to Pay program).

With regard to CTAs, China was the first country to introduce mobile contact tracing as a means of curbing the spread of the COVID-19 virus, rolling out its Health Code app nationwide in February 2020. After registration, the app automatically collects travel and medical data, as well as self-reported travel histories, to assign users a red, yellow, or green QR code. A green code gives users unhindered access to public spaces, a yellow code indicates that the person might have come into contact with COVID-19 and, therefore, has to be confined to their homes, and a red code identifies users infected with the virus. As public spaces like shopping malls can only be accessed with a green QR code, installing the Health Code app became effectively mandatory in China, resulting in broad adoption of the app among Chinese citizens. By contrast, in Germany, the UK, and the US, CTAs were voluntary and predominantly based on Bluetooth technology. Germany launched its Corona-Warn-App in June 2020, after a drawn-out discussion over data privacy issues and the related design of the app. The app uses Bluetooth technology to track the distance and length of interpersonal encounters between people that carry a mobile phone with the app installed. In the US, rather than a top-down approach by the central government, state and local governments cooperated with Apple and Google to develop local apps (Fox Business, 2020; Johnson, 2020a). By the end of 2020, more than 30 states had adopted CTAs in the US (Johnson, 2020b). Like the

<sup>2</sup> For example, noncompliance with specific legal judgments may result in restrictions or a prohibition on purchasing luxury goods or using high-speed railways and airplanes (Knight and Creemers, 2021). By contrast, contributions to society, such as donations or volunteering activities, may be rewarded (Knight and Creemers, 2021).

German case, these apps rely on Bluetooth technology, their use is voluntary, and they notify users once they have been in close contact with infected persons for at least 5 min. They do not collect personal information and do not upload information about personal encounters to central servers (Kreps et al., 2020; Kostka and Habich-Sobieghalla, 2022).

#### 2.4. Analytical framework

This study takes as its dependent variable respondents who expressed doubts about digital technologies. Building on previous studies that report on acceptance levels, this article studies the groups that were more doubtful about these new technologies. In the analysis, two groups are identified. *Strong digital doubters* of digital technologies are individuals who either strongly or somewhat oppose the use of digital technology. The group of *digital doubters* of digital technology are individuals who either strongly, somewhat oppose, or neither accept nor oppose the use of digital technology. The answer option of “neutral” is included in the group of digital doubters as it is likely that respondents in China opted for a more neutral answer when they actually do harbor doubts about the digital technologies.<sup>3</sup> The explanatory variables, which are derived from the literature on surveillance, security-private trade-offs, and privacy calculus theory, are a range of perceived benefits and risks. Two hypotheses are tested:

**Hypothesis 1:** Digital doubters are citizens who are not aware or do not believe in the various *benefits* of digital technologies, such as convenience, security, and efficiency (H1).

**Hypothesis 2:** Digital doubters are citizens who are aware or believe in the various *risks* of digital technologies, such as surveillance, privacy violations, discrimination, and misuse (H2).

Trust in government, along with sociodemographic variables, is controlled for. Figure 1 summarizes the analytical framework.

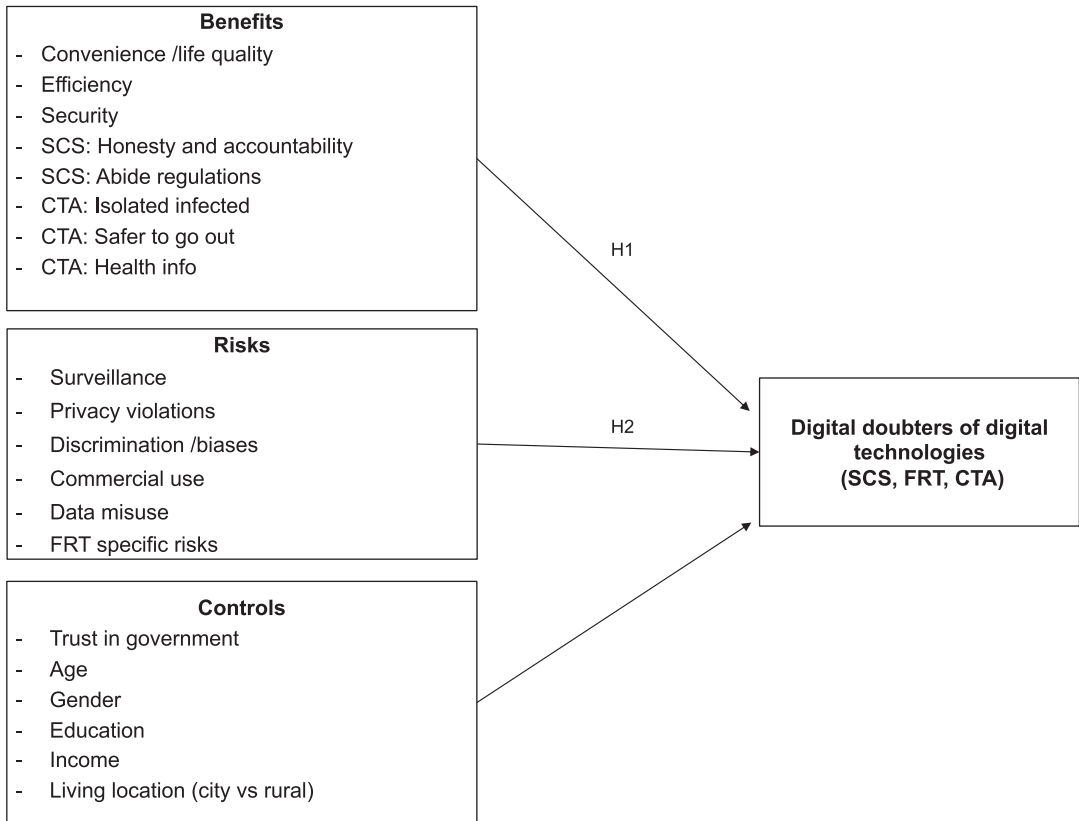
### 3. Data and Methods

This article looks at citizens’ attitudes toward major digital technologies in China, Germany, the UK, and the US by selecting SCSs (China only), FRT (all four countries), and CTAs (China, Germany, and the US only) as case studies. The analysis is based on three online surveys through one professional survey firm in 2018 (SCSs), 2019 (FRT), and 2020 (CTAs).<sup>4</sup> The survey company cooperated with app and mobile website providers. As a sampling method, we used river sampling, also referred to as intercept sampling or real-time sampling, to draw participants from a base of between 1 and 3 million unique users (Lehdonvirta et al., 2021).<sup>5</sup> This allowed both first-time and regular survey-takers to participate. From a network of more than 40,000 participating apps and mobile websites, the different surveys included respondents through more than 100 apps comprising different formats and topics such as shopping (e.g., Amazon), photo-sharing (e.g., Instagram), lifestyle (e.g., DesignHome), and messaging (e.g., Line) providers. Offer walls provided participants the options to receive small financial and nonmonetary rewards as an

<sup>3</sup> Neutral respondents are individuals who neither accept nor oppose to digital technology.

<sup>4</sup> This article combines three existing datasets published previously separately (Kostka, 2019; Kostka et al., 2021, 2023; Kostka and Habich-Sobieghalla, 2022; Guo et al., 2023). This results in a number of issues. First, the countries in the comparative analysis are not identical, for example, the UK is included for the FRT analysis but not in the CTA analysis. Second, the surveys were conducted in three different years. The different timing of the different surveys potentially influences the outcomes. Especially since the end of 2020, online criticism against the Suzhou “Civility Code” has increased public awareness about potential risks of digital technologies. In late 2020, after Chinese local governments had aggressively rolled out a variety of “health code” systems during the COVID-19 pandemic, a discussion emerged about the Suzhou Civility Code. Since the government had imposed draconian surveillance measures to contain the pandemic, citizens may have experienced a rising awareness about the aggressiveness of such surveillance systems, which could have contributed to the criticism against the civility code. Despite these two issues that arise due to merging existing surveys, we believe that the general argument about digital doubters is not affected.

<sup>5</sup> River sampling does not include a fixed number of potential survey respondents, as the survey is displayed on offer walls within apps and websites and can, thus, reach millions of users.



**Figure 1.** Analytical framework.

incentive to take part in our survey, such as premium content, extra features, vouchers, and PayPal cash. Users did not know the topic of the questionnaire before opting in to participate. Instead, each participant underwent a prescreening before being directed to a survey that they were a match for. [Table 1](#) summarizes the key features of each survey, and [Tables A1–A3](#) in the Supplementary Material provide further data on the sample. The Supplementary Material offers further details on the survey method, questionnaire design, and sample representativeness.

[Table 2](#) summarizes the measures and hypotheses for this article.

## 4. Results

### 4.1. Digital doubters across the three technologies

The findings show that in China, the group of digital doubters is largest when it comes to FRT: Here, 9% of the respondents stated they strongly or somewhat oppose the technology, compared with only 2% for SCSs and CTAs. The group of neutral respondents is also largest for FRT with 25%, as compared with 19% and 17% for SCSs and CTAs, respectively. The group of digital doubters (i.e., strong doubters and neutral group) is 34% for FRT, 21% for SCSs, and 19% for CTAs. The different rates of doubt suggest that Chinese citizens are less accepting of FRT, which matches a person's facial features from a digital image or video to identifying data. Interestingly, SCSs, which potentially covers a wider range of areas, has much lower rates of doubt. The lowest doubts are for CTAs, which could possibly be explained by the fact that during the pandemic, the perceived health benefits of CTAs have had a particularly strong effect on CTA acceptance in China (Kostka and Habich-Sobiegalla, 2022).

**Table 1.** Three online surveys on SCSs, FRT, and CTAs

	SCSs	FRT	CTAs
Survey time	February and April 2018	August and September 2019	June 2020
Methods	River sampling	River sampling	River sampling
Sample size	China: $n = 2,209$	China: $n = 1,651$ Germany: $n = 1,677$ UK: $n = 1,685$ US: $n = 1,620$	China: $n = 2,201$ Germany: $n = 2,083$ US: $n = 2,180$
Sampling methods	Sampled by age (18–65), gender, and China by region: Central, (37%), Western (21%), and Eastern (42%) <sup>a</sup>	Sampled by age (18–65), gender, and China by region: Central, (37%), Western (21%), and Eastern (42%) <sup>a</sup>	Sampled by age (18–65), gender, and China by region: Central, (37%), Western (21%), and Eastern (42%) <sup>a</sup>
Maximum weight	2.0	1.8	1.4
Overall margin of error (in %)	2.2	2.4	2.1

Abbreviations: CTAs, contact tracing apps; FRT, facial recognition technology; SCSs, social credit systems.

<sup>a</sup>Respondents in China were sampled by region; for the other three countries the sample provided by the survey company generally resembles the population and no additional regional sampling quota was needed.

The group of strong doubters in Germany is much larger than in China, with 32% for FRT and 27% for CTAs. A third of the respondents hold a neutral attitude toward these two technologies, making the group of digital doubters 63% for FRT and 60% for CTAs. The high level of doubt regarding the German Corona-Warn-App is surprising, as during the design phase, numerous adjustments were made to address Germans' high levels of privacy concerns, but the findings suggest that doubts remain. In the UK and the US, we find the group of strong digital doubters is slightly smaller than in Germany, with 23% strong doubters in the UK for FRT and 26% strong doubters in the US for FRT and 22% for CTAs. Table 3 summarizes this data.

#### 4.2. Explanatory factors

We assessed the association between our predictor variables and digital technology doubts for the three different technologies by using logit regressions for a binary outcome dependent variable. We ran two models for each technology and used two dependent variables: strong doubters and digital doubters. In the model with strong doubters as the dependent variable, we coded respondents who either strongly or somewhat oppose a particular digital technology as 1, the others as 0. In the model with digital doubters as the dependent variable, we coded respondents who either strongly or somewhat oppose (or have a neutral opinion toward) a certain technology as 1, the others as 0. Trust in government and sociodemographic factors are included as control variables for each of the three technologies. The exponentiated coefficients in the graphics and regression tables indicate the odds ratio (OR). When  $0 < OR < 1$ , it implies a negative relationship between the explanatory variable and the dependent variable; when  $OR > 1$ , it implies a positive relationship.

In line with our benefits–risks analytical framework, the different models measure the effects of different benefits (e.g., convenience, efficiency, security, improved regulations, isolation of COVID-infected) and risks (e.g., surveillance, privacy violations, discrimination /biases, data misuse). Tables A1–A5 in the Supplementary Material present the regression tables and additional information about the fit of the logistic regression model, including results for the VIF.



**Table 2.** Measurement table and hypotheses

Variable	Measurement
<i>Dependent variable—Doubters of digital technologies</i>	
Doubters	Doubters include individuals whose attitudes toward technologies under investigation are either (a) strongly disapproving/opposing, (b) somewhat disapproving/opposing, or (c) neutral 0 = No doubters, 1 = Doubters
Strong doubters	Strong doubters include individuals whose attitudes toward technologies under investigation are either (a) strongly disapproving/opposing or (b) somewhat disapproving/opposing 0 = No strong doubters, 1 = Strong doubters
<i>Benefits</i>	
<i>Hypothesis 1. People who are not aware of and do not believe in the benefits of digital technologies are more likely to be digital doubters</i>	
Convenience/life quality	SCS: I do not mind that my personal information is collected and assessed if the social credit system improves the overall quality of my life 1 = Strongly disagree, 2 = Somewhat disagree, 3 = Neither agree nor disagree, 4 = Somewhat agree, 5 = Strongly agree <i>Dummy: 0 = prefer life quality; 1 = prefer privacy</i> What is more important to you when using mobile payment apps: convenience or privacy? <i>5-point sliding scale: 1 = mostly convenience, 3 = both equally, 5 = mostly privacy</i> <i>Dummy: 0 = more convenience/same; 1 = more privacy</i> FRT: Do you think FRT increases any of the following? <i>Among others...</i>
Efficiency	Convenience—0 = No, 1 = Yes FRT: Do you think FRT increases any of the following? <i>Among others...</i>
Security	Efficiency—0 = No, 1 = Yes FRT: Do you think FRT increases any of the following? <i>Among others...</i>
SCS-specific benefits	Security—0 = No, 1 = Yes SCS: [honesty and accountability] “A social credit system is a useful tool to make individuals and companies more honest and accountable for their actions” 1 = Strongly disagree, 2 = Somewhat disagree, 3 = Neither agree nor disagree, 4 = Somewhat agree, 5 = Strongly agree <i>Dummy: 0 = Increase in accountability, 1 = No increase in accountability</i> [abide by regulations] How helpful are social credit systems in ensuring that companies abide by regulations (e.g., regarding ecological standards and product quality requirements)? 1 = Not at all helpful, 2 = Not very helpful, 3 = Somewhat helpful, 4 = Very helpful, 5 = Do not know <i>Dummy: 0 = Helpful with obeying rules, 1 = Not helpful with obeying rules</i>
CTA-specific benefits	CTA: Do you believe that the use of COVID-19 tracing apps would result in any of the following? <i>Among others...</i> Fewer infections—0 = No, 1 = Yes

(Continued)

**Table 2.** *Continued*

Variable	Measurement
	Isolate infected people—0 = No, 1 = Yes Safer to go out—0 = No, 1 = Yes Better health information—0 = No, 1 = Yes
Risks	<i>Hypothesis 2: People who are aware of and believe in the risks of digital technologies are more likely to be digital doubters</i>
Surveillance	<i>CTA: Do you believe that the use of COVID-19 tracing apps would result in any of the following?</i> <i>Among others...</i> Government surveillance—0 = No, 1 = Yes <i>FRT: Do you think FRT increases any of the following?</i> <i>Among others...</i> Surveillance—0 = No, 1 = Yes
Privacy violation	<i>SCS: See convenience/quality of life in the category of benefits</i> <i>CTA: Do you believe that the use of COVID-19 tracing apps would result in any of the following?</i> <i>Among others...</i> Privacy violations—0 = No, 1 = Yes <i>FRT: Do you think FRT increases any of the following?</i> <i>Among others...</i> Privacy violation—0 = No, 1 = Yes Do you think FRT poses a threat to your privacy? 1 = No, 2 = Maybe, 3 = Yes, 99 = do not know Dummy: 0 = No/Maybe/Do not know, 1 = Yes
Discrimination/biases	<i>SCS: Do you think your credit score is fairly calculated? 1 = Very unfair, 2 = Somewhat unfair, 3 = Somewhat fair, 4 = Very fair, 99 = I do not know</i> Dummy: 0 = fair/do not know, 1 = unfair “Machine learning algorithms are less biased than human judgments when calculating social credit scores” 1 = Strongly disagree, 2 = Somewhat disagree, 3 = Neither agree nor disagree, 4 = Somewhat agree, 5 = Strongly agree Dummy: 0 = Machine learning less biased, 1 = Machine learning not less biased <i>CTA: Do you believe the use of COVID-19 tracing apps will result in any of the following?</i> <i>Among others...</i> Discrimination against people who test positive—0 = No, 1 = Yes <i>FRT: Do you think FRT increases any of the following?</i> <i>Among others...</i> Discrimination—0 = No, 1 = Yes
Commercial use	<i>CTA: Do you believe the use of COVID-19 tracing apps will result in any of the following?</i> <i>Among others...</i> Use of data for commercial purpose—0 = No, 1 = Yes
Data misuse	<i>SCS: How much control do you feel you have over how your personal information online is used by others?</i> 1 = None at all, 2 = Not a lot, 3 = A little, 4 = A lot

*(Continued)*

Table 2. Continued

Variable	Measurement
	99 = Do not know Dummy: 0 = a lot of control/do not know 1 = none/not a lot/a little
FRT-specific risks	FRT: In which of the following situations do you think someone will likely experience negative consequences? Among others... Citizens refuse to scan—0 = No, 1 = Yes False identification—0 = No, 1 = Yes Leaking of facial data—0 = No, 1 = Yes Failure to detect—0 = No, 1 = Yes In general, do you think facial recognition technology comes with more risks or more benefits? 1 = More risks, 2 = Slightly more risks, 3 = Neither more risks nor more benefits, 4 = Slightly more benefits, 5 = More benefits Dummy: 0 = More benefits/same, 1 = More risks
<i>Trust in government (control variable)</i>	
Trust in government/ confidence	SCSs: How much confidence do you have in the way the current government is running the country? 1 = full confidence, 2 = quite a lot of confidence, 3 = not very much confidence, 4 = no confidence at all For FRT and CTAs: How much do you trust your country's government institutions? FRT: 1 = a lot, 2 = somewhat, 3 = very little, 4 = not at all CTA: 1 = a lot, 2 = somewhat, 3 = neither trust nor distrust, 4 = not much, 5 = not at all
<i>Sociodemographics (control variable)</i>	
Age	For SCSs: 14–64 For FRT and CTAs: 18–65 Age groups for SCSs: 14–30, 31–50, 51–64 Age groups for FRT and CTA: 18–35, 35–50, 51–65
Gender	0 = Male, 1 = Female
Education <sup>a</sup>	1 = Low (no formal education), 2 = Medium (high school or equivalent), 3 = High (university degree)
Income	1 = Low (<1,000), 2 = Medium (1,000–4,000), 3 = High (>4,000), 4 = No answer
Location	Current living location: 0 = Rural, 1 = City

Abbreviations: CTAs, contact tracing apps; FRT, facial recognition technology; SCSs, social credit systems.

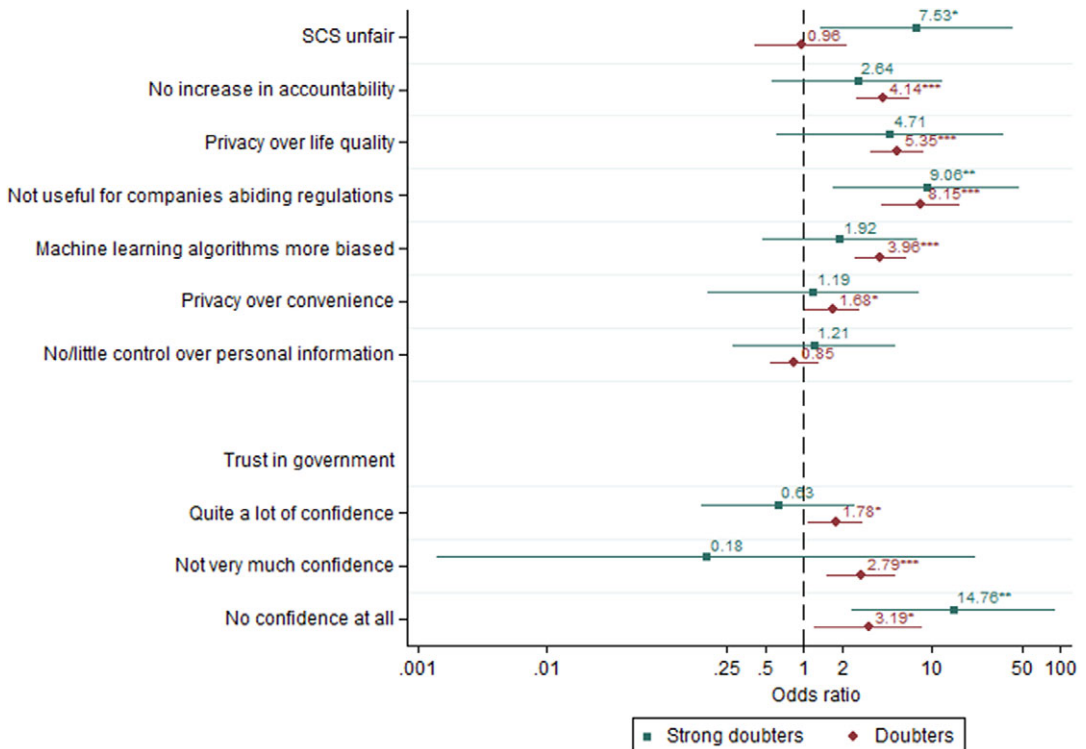
<sup>a</sup>Low level includes: no formal education; medium level includes: high school or equivalent and vocational training; high level includes: bachelor's degree and above.

Numerous factors explain why a small group of citizens are doubtful of SCSs, as illustrated in Figure 2. Among the group of people who have strong doubts about SCSs, the most significant predictor is a belief that SCSs is not useful for pressuring companies to abide by regulations (positive odds ratio of 9.06). We also find a positive significant association between strong doubts about SCSs and the belief that SCSs are unfair. Furthermore, we find a significant positive association between respondents who have no confidence in the Chinese government and being strong doubters. In the model with digital doubters as the dependent variable, all groups with less confidence in the government show positive significant outcomes, with the “no confidence at all” group having the largest odds ratio. In other words, the less trust in the government there is, the more likely a respondent is to belong to the group of digital doubters. All

**Table 3.** Number of strong doubters and doubters in the population

		SCSs	FRT	CTAs
China	Sample size	2,209	1,651	2,201
	Strong doubters	2% (n = 30)	9% (n = 141)	2% (n = 55)
	Neutral	19% (n = 415)	25% (n = 417)	17% (n = 370)
	Digital doubters	21% (n = 445)	34% (n = 558)	19% (n = 425)
Germany	Sample size		1,677	2,083
	Strong doubters		32% (n = 534)	27% (n = 557)
	Neutral		31% (n = 525)	33% (n = 683)
	Digital doubters		63% (n = 1,060)	60% (n = 1,240)
UK	Sample size		1,685	
	Strong doubters		23% (n = 387)	
	Neutral		30% (n = 499)	
	Digital doubters		53% (n = 885)	
US	Sample size		1,620	2,180
	Strong doubters		26% (n = 427)	22% (n = 486)
	Neutral		29% (n = 473)	38% (n = 839)
	Digital doubters		56% (n = 899)	61% (n = 1,326)

Note: Strong doubters of digital technology are individuals who either *strongly* or *somewhat* oppose the use of digital technology. Neutral respondents are individuals who neither accept nor oppose digital technology. Digital doubters are individuals who are either strong doubters or neutral. Abbreviations: CTAs, contact tracing apps; FRT, facial recognition technology; SCSs, social credit systems.



**Figure 2.** Odds ratios of effects on digital doubters' concerns about social credit systems (SCSs). \*p < 0.05, \*\*p < 0.01, and \*\*\*p < 0.001.

other predictor variables and control variables are not significant, with the exception of the positive significant relation for education and income in the digital doubters group. In sum, strong doubters in SCSs believe the SCS system itself is not effective or unfair.

Disbelief in the benefits of FRT also explains the attitude of respondents with strong doubts about FRT. With the exception of Germany for convenience and the UK for efficiency, the results in Figure 3 show a significant negative relationship between a doubting attitude toward FRT and beliefs in convenience and efficiency. In other words, digital doubters do not believe FRT offers more convenience and efficiency. For all four countries, there is also a negative significant association between doubts toward FRT and security, which suggests that digital doubters do not believe that a more widespread adoption of FRT results in advanced security. Except for China, the digital doubter group also believes FRT can result in privacy violations, and therefore, they are more doubtful. With regard to surveillance, the results are mixed. For China, there is a positive relationship between perceived surveillance and the likelihood to be strong doubters. For the UK, we find no significant relationship between whether respondents believe FRT will result in more surveillance and being a digital doubter. However, the results for Germany and the US are slightly surprising. We find that respondents who perceive FRT will increase surveillance are less likely to be digital doubters in Germany and less likely to be strong digital doubters in the US (significant negative association). One possible explanation might be that people have different positive or negative associations with surveillance, and some respondents might have associated surveillance with increased public security. Overall, in all four countries, respondents find that FRT generally has more risks than benefits. Overall, the sociodemographic control variables are not significant, except for age in China (positive), gender in Germany and the UK (positive), education in Germany and the US (negative), and income (negative for doubters in China and positive for strong doubters in Germany). In sum, one of the

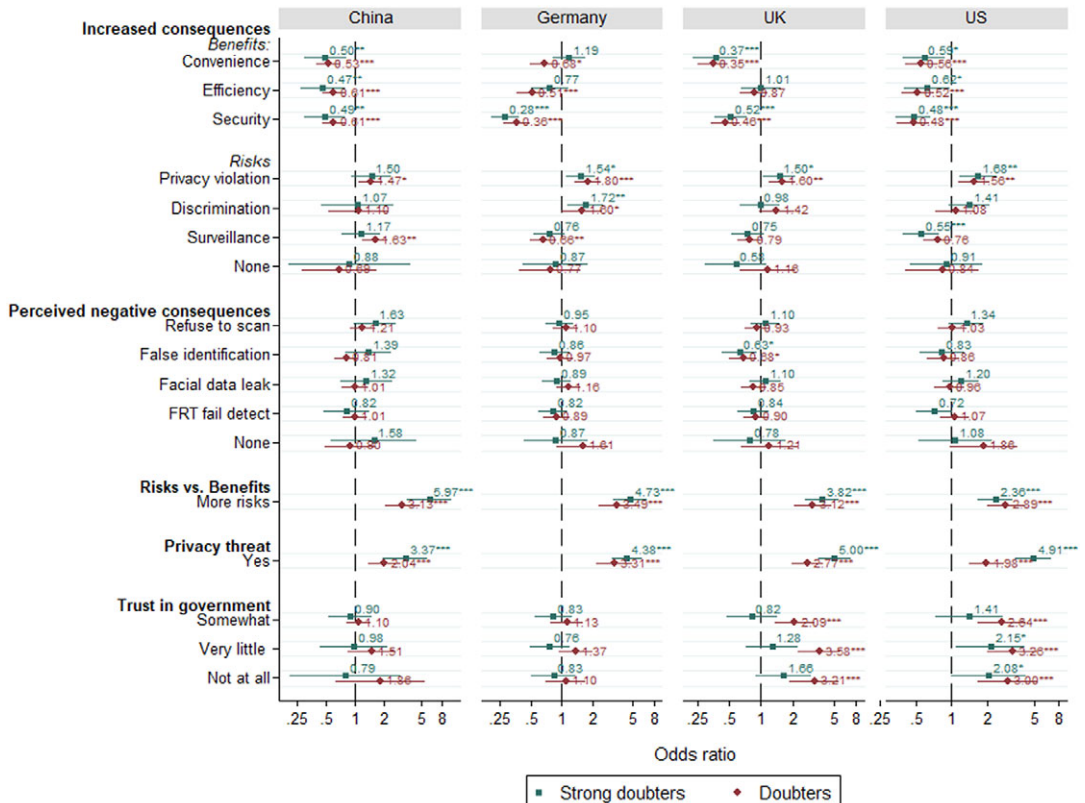
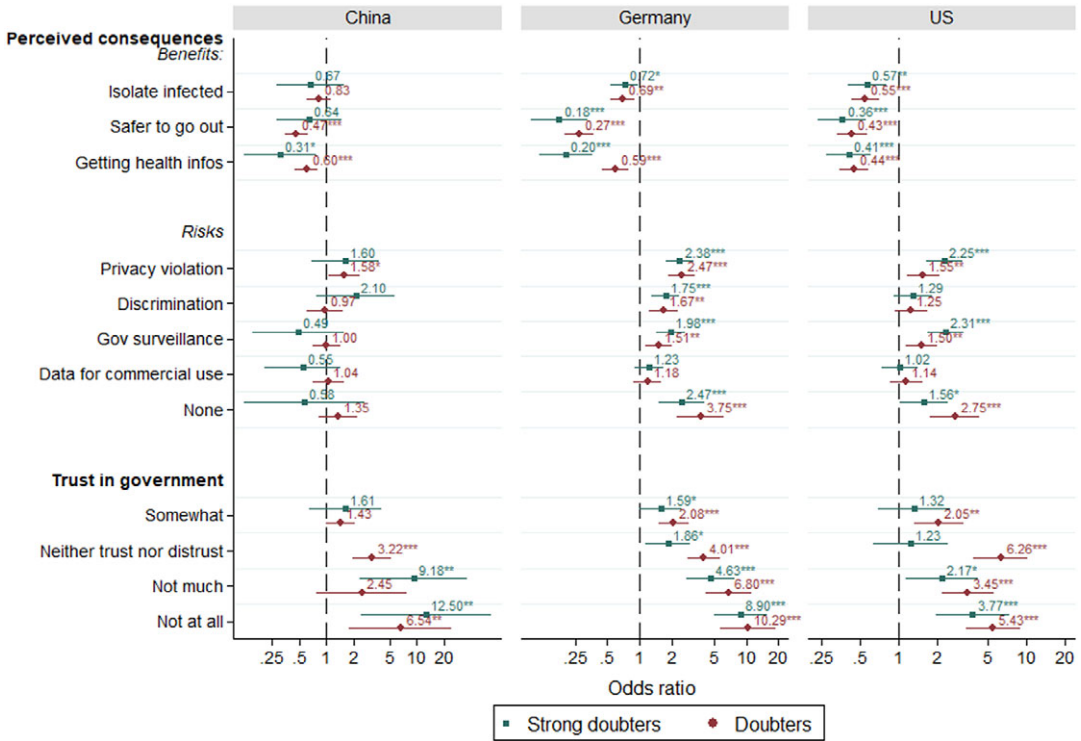


Figure 3. Odds ratios of effects on digital doubters' concerns about facial recognition technology (FRT).



**Figure 4.** Odds ratios of effects on digital doubters' concerns about contact tracing apps. \*p < 0.05, \*\*p < 0.01, and \*\*\*p < 0.001.

strongest indicators of being doubtful about FRT is a belief that the technology increases security or not. At the same time, the more risks someone associates with FRT, including privacy violations, the more likely they are to be a digital doubter.

The analysis of CTAs also finds that strong doubters do not believe in FRT having particular benefits. Figure 4 shows that in China, Germany, and the US, there is a negative, significant relation between strong doubters and the CTAs offering health information. In all three countries, respondents who believe CTAs do not make it safer for people to go out are more likely to belong to the group of digital doubters. In the US and Germany, the lack of a belief that CTAs help isolate infected people also helps explain doubts about the CTAs. The German and US citizens who perceive that CTAs will result in privacy violations and government surveillance are more likely to be digital doubters. In China, those who think that CTAs will result in more privacy violations are more likely to be strong digital doubters. Respondents who distrust the government somewhat or a lot are also likely to be digital doubters, as we find a positive significant association in all three countries with those that do not trust the government much or at all. Socio-demographic control variables are mostly insignificant, except for age in Germany (negative association), gender in Germany (negative association), education in China and the US (negative association), and income levels in China and Germany (negative association).

**4.3. Research limitations**

The analysis is subject to a number of limitations. First, as this was an online survey using mobile phones and desktops, the findings can only reflect the views of the Internet-connected population in the selected countries. Second, respondents who chose to participate in online surveys may already have a particular affinity for technology, which could positively affect their stance toward innovations in this field, and the group of digital doubters might actually be larger than reported here. This effect may have been

exacerbated by the virtual rewards individuals were promised for participating, since they might have been more likely to associate the positivity of incentives with positivity toward digital technology. Third, as the study combined three datasets, the respondents' attitudes toward the three technologies cannot be directly compared. In the future, it would be helpful to conduct one larger survey rather than combining three datasets.

Furthermore, China's authoritarian political context makes it difficult to express dissent against technologies that are officially endorsed by the government, and this might be reflected in the reported levels of technology nonacceptance in this study. Although participants were aware that any identifying data was anonymized and analyzed for research purposes only, we cannot exclude the possibility of preference falsification as some more cautious respondents may have given false answers due to concerns over possible reprisals from the state. For instance, variables like attitudes toward surveillance might actually be underreported.

## 5. Conclusion

Governments around the world are embracing digital technologies for information collection, governance, and social control. Recent studies suggest citizens in both democratic and authoritarian regimes may accept or even support the adoption of digital technologies for governance purposes, despite their clear surveillance potential (Xu, 2019; Kostka et al., 2021; Liu, 2021; Xu et al., 2022). Using an online survey dataset on the public's opinion of digital technologies in China, Germany, the UK, and the US, this article shows that these findings overlooked a small yet significant group of digital technology doubters. The analysis looks at citizens' attitudes toward three major digital technologies in China: FRT, CTAs, and SCSs. The findings show that the group of "digital doubters" is largest in Germany, followed by the UK and the US, and smallest in China.

For all three technologies, we find that digital doubters are engaging in a cost–benefit calculus, which results in them rating the benefits lower than the risks. Respondents who belonged to the group of strong doubters are not convinced of the effectiveness and usefulness of digital technologies, including benefits such as greater convenience, efficiency, or security. The doubting attitudes are also associated with concerns about technology risks, especially privacy risks and surveillance threats. The findings add to the privacy calculus literature (Dinev and Hart, 2006) and highlight that digital doubters are more often skeptics because they do not believe in the perceived benefits. Our findings show that in both democratic and authoritarian states, there are citizens opposing the adoption of certain digital technologies. This underlines the importance of initiating societal debate to determine the appropriate regulations that align with these societal preferences.

Interestingly, in China, FRT, which matches a person's facial features from a digital image or video with identifying data, raises more doubts than SCSs that potentially cover a wider range of areas in society. Doubts toward FRT might be higher as access to biometric data is a more *visible* intrusion of privacy violations than local governments' collection of a variety of personal data as part of local SCSs. Recent research shows that SCSs predominantly target businesses and not individuals (Krause and Fischer, 2020) and that, if they are affected by these SCSs, citizens interpret the SCS more as a regulatory tool to reinforce the social order (Kostka, 2019). Comparatively lower rates of doubt toward CTAs could possibly be explained by the fact that the technology came into use during the COVID-19 pandemic, with the pandemic offering a public health justification for technology adoption.

Finally, the impact of China's digital technology entails more than its domestic influence as China has exported its information technology and potentially digital authoritarianism for years. With the country's increasingly ability to utilize digital technology as both high-tech export goods and foreign policy strategy tools, observers worry that if liberal democracies fail to offer a compelling and cost-effective alternative, the Chinese style of digital governance will spread fast around the globe (Polyakova and Meserole, 2019). Various countries are embracing the Chinese-style digital authoritarianism of extensive censorship and automated surveillance systems (Shahbaz, 2018). For instance, AI-powered surveillance has been deployed most sweepingly in repression in China such as online censorship and in Xinjiang, with other

countries following suit (Kendall-Taylor et al., 2020). Therefore, the study of digital doubters within China not only remains theoretically intriguing but could also offer important implications for other digitalizing countries.

**Supplementary material.** The supplementary material for this article can be found at <https://doi.org/10.1017/dap.2023.25>.

**Acknowledgments.** The author is very grateful for excellent research support from Danqi Guo.

**Funding statement.** Funding was provided by the European Research Council (ERC Starting Grant No: 852169) and the Volkswagen Foundation Planning Grant on “State-Business Relations in the Field of Artificial Intelligence and its Implications for Society” (Grant 95172).

**Competing interest.** The author declares no competing interests.

**Author contribution.** Conceptualization: G.K.; Data curation: G.K.; Funding acquisition: G.K.; Investigation: G.K.; Methodology: G.K.; Project administration: G.K.; Resources: G.K.; Writing—original draft: G.K.; Writing—review and editing: G.K.

**Data availability statement.** The data that support the findings are available via the author’s institutional repository: <http://doi.org/10.17169/refubium-39987>

## References

- Acquisti A and Grossklags J** (2005) Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine* 3 (1), 26–33. <https://doi.org/10.1109/MSP.2005.22>
- Article 19** (2021) Emotional entanglement: China’s emotion recognition market and its implications for human rights. *Article 19*, January. Available at <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf> (accessed 6 July 2022).
- Bodo B, Heberger N, Irion K, Zuiderveen Borgesius F, Moller J, van de Velde B, Bol N, van Es B and de Vreese C** (2017) Tackling the algorithmic control crisis—the technical, legal, and ethical challenges of research into algorithmic agents. *The Yale Journal of Law & Technology* 19, 133–180.
- Brayne S** (2017) Big data surveillance: The case of policing. *American Sociological Review* 82(5), 977–1008. <https://doi.org/10.1177/0003122417725865>
- Brown TG, Statman A and Sui C** (2021) Public debate on facial recognition technologies in China. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. <https://doi.org/10.21428/2c646de5.37712c5c>
- Burrell J** (2016) How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society* 3(1), 205395171562251. <https://doi.org/10.1177/2053951715622512>
- Bushwick S** (2022) Russia is using ‘Digital Repression’ to suppress dissent. *Scientific American*, March 15. Available at <https://www.scientificamerican.com/article/russia-is-using-digital-repression-to-suppress-dissent/> (accessed 31 July 2023).
- Chadwick A** (2003) Bringing E-democracy back in: Why it matters for future research on E-governance. *Social Science Computer Review* 21(4), 443–455. <https://doi.org/10.1177/0894439303256372>
- Chiu K** (2020) Suzhou city takes a page from China’s social credit system with Civility Code that rates citizens’ behaviour through a smartphone app. *South China Morning Post*, September 8. Available at <https://www.scmp.com/abacus/tech/article/3100516/suzhou-city-takes-page-chinas-social-credit-system-civility-code-rates> (accessed 31 July 2023).
- Chorzempa M, Triolo P and Sacks S** (2018) *China’s Social Credit System: A Mark of Progress or a Threat to Privacy?* (No. PB18-14). Peterson Institute for International Economics. Available at <https://ideas.repec.org/p/iie/pbrief/pb18-14.html> (accessed 31 July 2023).
- Citron DK and Pasquale F** (2014) The scored society: Due process for automated predictions. *Washington Law Review* 89(1), 1–33.
- Creemers R** (2017) Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China* 26(103), 85–100. <https://doi.org/10.1080/10670564.2016.1206281>
- Creemers R** (2018). China’s Social Credit System: An evolving practice of control. SSRN. Retrieved from: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3175792](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792), (accessed 31 July 2023).
- Dai X** (2018) Toward a reputation state: The social credit system project of China. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3193577>
- Davenport C** (2007) State repression and the tyrannical peace. *Journal of Peace Research* 44(4), 485–504. <https://doi.org/10.1177/0022343307078940>
- Davis DW and Silver BD** (2004) Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science* 48(1), 28–46. <https://doi.org/10.1111/j.0092-5853.2004.00054.x>
- Deibert R** (2015) Cyberspace under siege. *Journal of Democracy* 26(3), 64–78. <https://doi.org/10.1353/jod.2015.0051>
- Diakopoulos N** (2015) Algorithmic accountability: Journalistic investigation of computational power structures. *Digital Journalism* 3(3), 398–415. <https://doi.org/10.1080/21670811.2014.976411>



- Dinev T and Hart P** (2006) An extended privacy calculus model for E-commerce transactions. *Information Systems Research* 17 (1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
- Downs ES and Saunders PC** (1999) Legitimacy and the limits of nationalism: China and the Diaoyu Islands. *International Security* 23(4), 114–146.
- Du X** (2020) Suzhou backtracks on ‘Civility Code’ for monitoring residents. *Sixth Tone*, September 7. Available at <https://www.sixthtone.com/news/1006151/suzhou-backtracks-on-civility-code-for-monitoring-residents> (accessed 31 July 2023).
- Earl J, Maher TV and Pan J** (2022) The digital repression of social movements, protest, and activism: A synthetic review. *Science Advances* 8(10), eabl8198. <https://doi.org/10.1126/sciadv.abl8198>
- Engelmann S, Chen M, Fischer F, Kao C and Grossklags J** (2019) Clear sanctions, vague rewards: How China’s social credit system currently defines “good” and “bad” behavior. In *Proceedings of the Conference on Fairness, Accountability, and Transparency*. Atlanta, GA: ACM, pp. 69–78. <https://doi.org/10.1145/3287560.3287585>
- Fox Business** (2020) Google, Apple release coronavirus contact-tracing technology for apps. *Fox Business*, May 20. Available at <https://www.foxbusiness.com/technology/apple-google-release-coronavirus-technology> (accessed 31 July 2023).
- Frantz E, Kendall-Taylor A and Wright J** (2020) *Digital Repression in Autocracies* (No. 27). V-Dem Institute at the University of Gothenburg.
- Gan N** (2019). The complex reality of China’s social credit system: hi-tech dystopian plot or low-key incentive scheme? South China Morning Post. Retrieved from The complex reality of China’s social credit system: hi-tech dystopian plot or low-key incentive scheme? (accessed 31 July 2023).
- Gandomi A and Haider M** (2015) Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management* 35(2), 137–144. <https://doi.org/10.1016/j.ijinfomgt.2014.10.007>
- Gerschewski J** (2013) The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes. *Democratization* 20(1), 13–38. <https://doi.org/10.1080/13510347.2013.738860>
- Gohdes AR** (2014) *Repression in the Digital Age: Communication Technology and the Politics of State Violence*. Mannheim: University of Mannheim.
- Guo D, Habich-Sobiegalla S, & Kostka G** (2023). Emotions, crisis, and institutions: Explaining compliance with COVID-19 regulations. *Regulation & Governance*. Retrieved from <https://doi.org/10.1111/rego.12509>
- Gunitsky S** (2015) Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics* 13(1), 42–54. <https://doi.org/10.1017/S1537592714003120>
- Guriev S and Treisman D** (2019) Informational autocrats. *Journal of Economic Perspectives* 33(4), 100–127. <https://doi.org/10.1257/jep.33.4.100>
- Harwell D** (2019) This facial recognition website can turn anyone into a cop—Or a stalker. *Washington Post*, July 7. Available at <https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/> (accessed 31 July 2023).
- Höchtel J, Parycek P and Schöllhammer R** (2016) Big data in the policy cycle: Policy decision making in the digital era. *Journal of Organizational Computing and Electronic Commerce* 26(1–2), 147–169. <https://doi.org/10.1080/10919392.2015.1125187>
- Holbig H and Gilley B** (2010) Reclaiming legitimacy in China: Holbig/Gilley/reclaiming legitimacy in China. *Politics & Policy* 38 (3), 395–422. <https://doi.org/10.1111/j.1747-1346.2010.00241.x>
- Huang L, Lu Y and Li Q** (2020) Information dilemma: China tries to balance convenience, personal privacy. *Global Times*, November 26. Available at <https://www.globaltimes.cn/content/1208095.shtml> (accessed 31 July 2023).
- Ji J, Guo X, Zhang M and Feng C** (2018) 人脸识别技术在高速公路打逃中的应用探讨 [Pinyin: Rén liǎn shíbié jìshù zài gāosù gōnglù dǎ táo zhōng de yìngyòng tàntǎo, English: Discussion on Application of Face Recognition Technology in Highway [Toll] Evasion]. 中国交通信息化 [Pinyin: zhōngguó jiāotōng xīnxi huà, English: China ITS Journal].
- Johnson B** (2020a) The Covid tracing tracker: What’s happening in coronavirus apps around the world. *MIT Technology Research*, December 6. Available at <https://www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker#usa-data> (accessed 31 July 2023).
- Johnson K** (2020b) Apple and Google say 25 states and territories have explored using COVID-19 contact tracing apps. *Venture Beat*, September 1. Available at <https://venturebeat.com/2020/09/01/apple-and-google-say-25-states-and-territories-have-explored-using-covid-19-contact-tracing-apps/> (accessed 31 July 2023).
- Kendall-Taylor A, Frantz E and Wright J** (2020) The digital dictators: How technology strengthens autocracy. *Foreign Affairs* 99 (2), 103–115. Available at <https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators> (accessed 31 July 2023).
- Kostka G** (2019) China’s social credit systems and public opinion: Explaining high levels of approval. *New Media & Society* 21(7), 1565–1593. <https://doi.org/10.1177/1461444819826402>
- Kostka G and Habich-Sobiegalla S** (2022) In times of crisis: Public perceptions toward COVID-19 contact tracing apps in China, Germany, and the United States. *New Media & Society*. <https://doi.org/10.1177/14614448221083285>
- Kostka G, Steinacker L and Meckel M** (2021) Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science* 30(6), 671–690. <https://doi.org/10.1177/09636625211001555>
- Kostka G, Steinacker L and Meckel M** (2023) Under big Brother’s watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly* 40(1), 101761.
- Knight A and Creemers R** (2021), Going Viral: The Social Credit System and COVID-19, Available at SSRN: <https://ssrn.com/abstract=3770208> or <http://doi.org/10.2139/ssrn.3770208>, (accessed 31 July 2023).

- Kraemer F, van Overveld K and Peterson M** (2011) Is there an ethics of algorithms? *Ethics and Information Technology* 13(3), 251–260. <https://doi.org/10.1007/s10676-010-9233-7>
- Krasnova H, Spiekermann S, Koroleva K and Hildebrand T** (2010) Online social networks: Why we disclose. *Journal of Information Technology* 25(2), 109–125. <https://doi.org/10.1057/jit.2010.6>
- Krause T and Fischer D** (2020) An economic approach to China's social credit system. In Everling O (ed), *Social Credit Rating*. Wiesbaden: Springer Fachmedien Wiesbaden, pp. 437–453. [https://doi.org/10.1007/978-3-658-29653-7\\_22](https://doi.org/10.1007/978-3-658-29653-7_22)
- Kreps S, Zhang B and McMurry N** (2020) Contact-tracing apps face serious adoption obstacles. *TechStream*, May 20. Available at <https://www.brookings.edu/techstream/contact-tracing-apps-face-serious-adoption-obstacles/> (accessed 31 July 2023).
- Laufer RS and Wolfe M** (1977) Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33(3), 22–42. <https://doi.org/10.1111/j.1540-4560.1977.tb01880.x>
- Lee C, Chang K and Berry FS** (2011) Testing the development and diffusion of E-government and E-democracy: A global perspective. *Public Administration Review* 71(3), 444–454. <https://doi.org/10.1111/j.1540-6210.2011.02228.x>
- Lehdonvirta V, Oksanen A, Räsänen P and Blank G** (2021) Social media, web, and panel surveys: Using non-probability samples in social and policy research. *Policy & Internet* 13(1), 134–155. <https://doi.org/10.1002/poi.3238>
- Lepri B, Staiano J, Sangokoya D, Letouzé E and Oliver N** (2017) The tyranny of data? The bright and dark sides of data-driven decision-making for social good. In Cerquittelli T, Quercia D and Pasquale F (eds), *Transparent Data Mining for Big and Small Data*. Cham: Springer International Publishing, pp. 3–24. [https://doi.org/10.1007/978-3-319-54024-5\\_1](https://doi.org/10.1007/978-3-319-54024-5_1)
- Li L** (2004) Political trust in rural China. *Modern China* 30(2), 228–258. <https://doi.org/10.1177/0097700403261824>
- Li J** (2019) How people in China are trying to evade Beijing's digital surveillance. *Quartz*, August 6. Available at <https://qz.com/1659328/chinese-people-are-pushing-back-on-beijings-digital-surveillance/> (accessed 31 July 2023).
- Li H and Kostka G** (2022) Accepting but not engaging with it: Digital participation in local government-run social credit systems in China. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4066462>
- Liu C** (2021) *Chinese public's support for COVID-19 surveillance in relation to the West*. *SSRN Electronic Journal*. Available at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3799322](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3799322) (accessed 31 July 2023).
- Liu C** (2022) Who supports expanding surveillance? Exploring public opinion of Chinese social credit systems. *International Sociology* 37(3), 391–412. <https://doi.org/10.1177/02685809221084446>
- Mac Sithigh D and Siems M** (2019) The Chinese social credit system: A model for other countries? *The Modern Law Review* 82(6), 1034–1071. <https://doi.org/10.1111/1468-2230.12462>
- MacKinnon R** (2011) China's "Networked authoritarianism". *Journal of Democracy* 22(2), 32–46. <https://doi.org/10.1353/jod.2011.0033>
- Manion M** (2006) Democracy, community, trust: The impact of elections in rural China. *Comparative Political Studies* 39(3), 301–324. <https://doi.org/10.1177/0010414005280852>
- Mayer-Schönberger V and Cukier K** (2013) *Big Data: A Revolution that Will Transform how we Live, Work, and Think*. Boston: Houghton Mifflin Harcourt.
- Monahan T** (2018) The image of the smart city: Surveillance protocols and social inequality. In Watanabe Y (ed), *Handbook of Cultural Security*. Cheltenham: Edward Elgar Publishing, pp. 210–226. <https://doi.org/10.4337/9781786437747.00017>
- Mozur P** (2019) One month, 500,000 face scans: How China is using AI to profile a minority. *The New York Times*, April 4. Available at <https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html?mtrref=duckduckgo.com&gwh=3C8D9935326B7A8B091BC65B0213540B&gwt=pay&assetType=PAYWALL> (accessed 31 July 2023).
- Munger K, Bonneau R, Nagler J and Tucker JA** (2019) Elites tweet to get feet off the streets: Measuring regime social media strategies during protest. *Political Science Research and Methods* 7(04), 815–834. <https://doi.org/10.1017/psrm.2018.3>
- O'Neil C** (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, 1st Edn. New York: Crown.
- Park G** (2020) The changing wind of data privacy law: A comparative study of the European Union's general data protection regulation and the 2018 California consumer privacy act. *UC Irvine Law Review* 10(4), 1455–1490.
- Pasquale F** (2015) *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge: Harvard University Press.
- Pinker S** (2018) *Enlightenment Now: The Case for Reason, Science, Humanism, and Progress*. New York: Viking, an imprint of Penguin Random House LLC.
- Polyakova A and Meserole C** (2019) *Exporting Digital Authoritarianism: The Russian and Chinese Models* (Policy Brief, Democracy and Disorder Series). Washington, DC: Brookings Institution, pp. 1–22.
- Prakash A** (2018) Facial recognition cameras and AI: 5 countries with the fastest adoption. *Robotics Business Review*, December 21. Available at <https://www.roboticsbusinessreview.com/ai/facial-recognition-cameras-5-countries/> (accessed 31 July 2023).
- Radanliev P** (2023) Review and comparison of US, EU, and UK regulations on cyber risk/security of the current blockchain technologies: Viewpoint from 2023. *The Review of Socionetwork Strategies*. <https://doi.org/10.1007/s12626-023-00139-x>
- Roberts M** (2018) *Censored: Distraction and Diversion inside China's Great Firewall*. Princeton: Princeton University Press. <https://doi.org/10.23943/9781400890057>
- Roussi A** (2020) Resisting the rise of facial recognition. *Nature* 587(7834), 350–353. <https://doi.org/10.1038/d41586-020-03188-2>
- Satriano A** (2019) Police use of facial recognition is accepted by British Court. *The New York Times*, September 4. Available at <https://www.nytimes.com/2019/09/04/business/facial-recognition-uk-court.html> (accessed 31 July 2023).

- Shahbaz A** (2018) The rise of digital authoritarianism. *Freedom House*. Available at <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism> (accessed 31 July 2023).
- Srivastava SC and Teo TSH** (2009) Citizen trust development for E-government adoption and usage: Insights from young adults in Singapore. *Communications of the Association for Information Systems* 25, 359–378. <https://doi.org/10.17705/1CAIS.02531>
- Steinhardt HC, Holzschuh L and MacDonald AW** (2022) Dreading big brother or dreading big profit? Privacy concerns toward the state and companies in China. *First Monday*.
- Su Z, Xu X and Cao X** (2021) What explains popular support for government monitoring in China? *Journal of Information Technology & Politics* 19, 377–392. <https://doi.org/10.1080/19331681.2021.1997868>
- Tan N** (2020) Minimal factionalism in Singapore's People's action party. *Journal of Current Southeast Asian Affairs* 39(1), 124–143. <https://doi.org/10.1177/1868103420932684>
- Wang Z** (2005) Before the emergence of critical citizens: Economic development and political trust in China. *International Review of Sociology* 15(1), 155–171. <https://doi.org/10.1080/03906700500038876>
- Wang Z and Yu Q** (2015) Privacy trust crisis of personal data in China in the era of big data: The survey and countermeasures. *Computer Law & Security Review* 31(6), 782–792. <https://doi.org/10.1016/j.clsr.2015.08.006>
- Westin AF** (1996) Privacy in the workplace: How well does American law reflect American values? *Chicago-Kent Law Review* 72 (1), 271–283.
- Wright N** (2018) How artificial intelligence will reshape the global order. *Foreign Affairs*, July 10. Available at <https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order> (accessed 31 July 2023).
- Xu X** (2019) *The social costs of digital vs. in-person surveillance*. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3572138>
- Xu X, Kostka G and Cao X** (2022) Information control and public support for social credit systems in China. *The Journal of Politics* 84, 2230–2245. <https://doi.org/10.1086/718358>
- Yao-Huai L** (2005) Privacy and data privacy issues in contemporary China. *Ethics and Information Technology* 7(1), 7–15. <https://doi.org/10.1007/s10676-005-0456-y>
- Zhao S** (2004) *A Nation-State by Construction: Dynamics of Modern Chinese Nationalism*. Stanford, CA: Stanford University Press.
- Zhao D and Hu W** (2017) Les déterminants de la confiance du public dans le gouvernement: Données empiriques en provenance de la chine urbaine. *Revue Internationale Des Sciences Administratives* 83(2), 365–384. <https://doi.org/10.3917/risa.832.0365>
- Zheng Y** (1999) *Discovering Chinese Nationalism in China: Modernization, Identity, and International Relations*. Cambridge: Cambridge University Press.